POLÍTICA INSTITUCIONAL

Título	Código	Revisão	Data	Página
POLITICA DE SEGURANCA DA INFORMACAO	POL-DIR-007	006	28/11/2024	1 de 9

1. HISTÓRICO DA REVISÃO

- Quarta revisão aprovada pelo Conselho de Administração em 09/05/2023;
- Alterado o item 5.8.1 destruição e eliminação dos dados em 01/04/2024;
- Quinta revisão aprovada pelo Conselho de Administração em 07/05/2024;
- Adicionada o item 5.11 referências bibliográficas, sem alteração no conteúdo do documento em 28/11/2024;

2. OBJETIVO

- Tornar pública a política de segurança da informação adotada pela Unimed Sul Capixaba e seus Recursos Próprios, visando garantir os princípios básicos de integridade, confidencialidade, disponibilidade, autenticidade, e legalidade das informações da cooperativa.

3. AREA DE APLICAÇÃO

- Unimed Sul Capixaba e partes interessadas.

4. DEFINIÇÕES

- Colaborador - Empregados, estagiários, office boys/girls, menores aprendizes, que atuam na Cooperativa. Para fins de alcance de políticas corporativas, ficam incluídos;

- Prestadores - Cooperados, parceiros e rede credenciada;

- Equipamentos portáteis \ Dispositivos móveis - Qualquer equipamento eletrônico com atribuições de mobilidade, tais como: notebooks, smartphones e pen drives;

- Informação - Dados, processados ou não, contidos em qualquer meio, suporte ou formato, que podem ser utilizados para a produção e transmissão de conhecimento;

- Partes interessadas - Pessoas e as organizações que podem ser afetadas por um projeto ou empresa, de forma direta ou indireta, positiva ou negativamente;

- TI - Tecnologia da Informação.

5. DIRETRIZES

Sumário

5.1. INTRODUÇÃO

A segurança da informação é um dos assuntos mais importantes dentre as preocupações de qualquer empresa. Confidencialidade, integridade e disponibilidade da informação estão diretamente ligadas à segurança.

Este documento descreve um conjunto de instruções, orientações e práticas, visando garantir o sigilo das informações relacionadas aos processos, rotinas e contratos, especialmente daqueles referentes à assistência médica (prontuários, diagnósticos, resultados laboratoriais e de imagem).

Por definição dessa política, ficam todos os colaboradores, prestadores e partes interessadas cientes de que os acessos às informações e uso de recursos de comunicação, prontuário e sistemas serão monitorados.

5.2. PRINCÍPIOS

A segurança da informação na Unimed Sul Capixaba tem como princípios:

- Confidencialidade: Ativos de informação serão protegidos garantir o sigilo das informações relacionadas aos processos, rotinas e contratos, especialmente daqueles referentes à assistência médica (prontuários, diagnósticos, resultados laboratoriais e de imagem), é fundamental o sigilo por porte de todos as pessoas que, em virtude da atividade que desempenham, tenham acesso a essas informações;

- Integridade: O valor e a utilidade dos dados dependem em grande parte da alta direção, dos nossos colaboradores e profissionais de saúde, sendo de responsabilidade de todos na cadeia de processo: assegurar a autenticidade, integridade, originalidade, rastreabilidade, certificação e reconhecimento de autoria;

- Disponibilidade: Os dados precisam estar seguros e disponíveis para serem acessados a qualquer momento por usuário autorizados.

5.3. ACESSO A INFORMAÇÃO

A Unimed Sul Capixaba dispõe de recursos tecnológicos para que os dados armazenados em seus sistemas de gestão sejam protegidos de acessos indevidos. Todos os acessos aos sistemas só são possíveis com uso de senhas pessoais e intransferíveis, respeitando o perfil de acesso do colaborador e atividades fins, conforme item 5.6.1. O perfil de acesso será definido pelo gestor da área.

As informações e trabalhos intelectuais produzidos pelos colaboradores da Unimed Sul Capixaba pertencem à cooperativa, devendo ser mantidos à sua disposição, inclusive no caso de desligamento do autor do material, sendo vedado o seu descarte sem prévia autorização da cooperativa.

O parque de impressoras possui recurso para impressão segura (para as ilhas de impressão) e somente através de cartão de proximidade e/ou senha as impressões podem ser autorizadas para que não haja extravio de documentos impressos. Para impressões em impressoras de uso pessoal/individual, a medida de segurança adotada será a orientação aos colaboradores para que não deixem documentos impressos nas impressoras.

5.4. RESPONSABILIDADES

5.4.1. DOS COLABORADORES / PRESTADORES

- Comunicar ao seu superior imediato o conhecimento de qualquer irregularidade ou desvio;

- Cumprir as regras de proteção estabelecidas aos ativos de informação;

- Cumprir esta política de segurança, sob pena de incorrer nas sanções disciplinares e legais cabíveis;
- Manter o caráter sigiloso, pessoal e intransferível da senha de acesso aos recursos e sistemas;
- Não compartilhar, sob qualquer forma, informações confidenciais com outros que não tenham a devida autorização de acesso;
- Preservar a integridade e guardar sigilo das informações de que fazem uso, bem como zelar e proteger os respectivos recursos de processamento de informações;
- Respeitar a proibição de não usar, inspecionar, copiar ou armazenar programas de computador ou qualquer outro material, em violação da legislação de propriedade intelectual pertinente;
- Responder, por todo e qualquer acesso, aos recursos da Unimed Sul Capixaba bem como pelos efeitos desses acessos efetivados através do seu código de identificação, ou outro atributo para esse fim utilizado;
- Utilizar os Sistemas de Informações da Unimed Sul Capixaba e demais recursos somente para os fins previstos pela Área de Tecnologia da Informação e/ou contrato de trabalho.

5.4.2. DOS GESTORES

- Comunicar formalmente para área de TI o tipo de acesso que os seus colabores deverão ter, conforme atividade a ser desempenhada e sobre o bloqueio de acessos, no caso de desligamento;
- Garantir que toda a sua equipe compreenda e desempenhe a obrigação de proteger a Informação;
- Gerenciar e monitorar o cumprimento desta política de segurança, por parte de seus colaboradores, identificando os desvios praticados e adotando as medidas corretivas apropriadas;
- Impedir o acesso de empregados / terceiros desligados aos ativos de informações da empresa;
- Proteger em nível físico e lógico os ativos de informação e de processamento de dados relacionados com sua área de atuação.

5.5. SEGURANÇA DO AMBIENTE FÍSICO

5.5.1. ACESSO FÍSICO

Acesso físico refere-se à utilização de medidas de segurança física (passivas e ativas), e de protocolos de gerenciamento, projetados para impedir o acesso não autorizado as áreas e salvaguardá-los contraespionagem, sabotagem, atos de terrorismo, danos, furto e roubo. Seu objetivo visa saber quem tem acesso concedido, quando o acesso é concedido, para onde e por que ele é concedido.

Os perímetros de segurança deverão ser claramente definidos, a localização e a capacidade de resistência de cada perímetro dependerão dos requisitos de segurança dos ativos que processem ou armazenem dados, inclusive dados pessoais, existentes no interior do perímetro e dos resultados de avaliação de riscos previamente realizada.

O acesso aos ambientes que contenham ativos de informação em seu formato físico será definido por meio do Procedimento de Acesso Físico a Ambientes de Armazenamento de Dados (PR-INF-009).

5.5.2. ESTAÇÕES DE TRABALHO

Toda estação de trabalho é exclusivamente ferramenta de trabalho de nossos colaboradores e também é um importante componente de segurança, sendo assim, somente arquivos de uso profissional deverão ser mantidos nesses equipamentos.

Fica vedada a instalação, execução e utilização de qualquer aplicativo ou componente físico (hardware), não instalado previamente neste, mesmo os classificados como gratuitos (freeware). Somente softwares autorizados e licenciados poderão ser instalados nestes equipamentos. Estas atividades devem ser realizadas por um colaborador da equipe da Tecnologia da Informação.

Não é permitida a gravação/manutenção de arquivos de música (MP3 ou outros formatos), filmes, fotos e softwares com direitos autorais ou qualquer outro tipo de pirataria. Na evidência de qualquer uma dessas práticas, os respectivos arquivos removidos sem comunicação prévia.

5.5.3. EQUIPAMENTOS PORTÁTEIS / DISPOSITIVOS MÓVEIS

Todos os dispositivos móveis, que tenham acesso a sistemas e aplicativos são regidos por essa política, o colaborador que tiver este tipo de equipamento para execução de suas atividades, receberá um termo de responsabilidade onde poderá ser observada as regras específicas de utilização destes dispositivos. Abaixo seguem as responsabilidades dos colaboradores que utilizam esses tipos de dispositivos:

- Acesso não autorizado ao equipamento portátil / dispositivo móvel ou aos dados pessoais sob responsabilidade da organização devem ser imediatamente reportados à área tecnologia da informação;
- Os colaboradores devem reportar imediatamente a perda, furto ou roubo de equipamentos portáteis / dispositivos móveis utilizados para o trabalho;
- Os colaboradores não têm acesso modificar qualquer configuração dos equipamentos da organização;
- Os colaboradores não têm permissão de instalação de softwares nos equipamentos da organização.

Não é permitido o uso de equipamentos portáteis / dispositivos móveis particulares na rede corporativa da cooperativa.

5.5.4. SALA DE SERVIDORES/SERVIDORES

O acesso ao ambiente ou serviços disponíveis em servidores, é controlado e protegido. O acesso físico a sala de servidores é restrita a pessoas previamente autorizadas por meio de senha individual ou crachás eletrônicos. O ambiente ainda possui monitoramento por câmeras de vídeos e todo acesso físico só é realizado com o acompanhamento de um membro da equipe de Tecnologia da Informação.

5.5.5. REDE DE DADOS

Toda a rede está arquitetada sobre uma infraestrutura que garante alto desempenho e disponibilidade. Os componentes críticos da rede local são mantidos/armazenados das seguintes maneiras:

- Em salas protegidas com acesso físico e lógico controlado, sendo protegidos contra danos, furtos, roubos e intempéries;
- Em equipamentos específicos para tal armazenamento e distribuídos pelos andares da empresa, tendo acesso restrito por chaves que ficam sobre a responsabilidade da área de TI;

- A configuração de todos os ativos de processamento é averiguada quando da sua instalação inicial, para que sejam detectadas e corrigidas as vulnerabilidades inerentes à configuração padrão;

- A alimentação elétrica é feita através de dispositivos apropriados.

Mecanismos de segurança baseados em sistemas de proteção de acesso (firewall) são utilizados para proteger as transações entre redes externas e a rede interna.

5.5.6. PRONTUÁRIO FÍSICO (SAME)

O prontuário físico é composto por documentos que eventualmente não possam ser eletrônicos ou digitalizáveis, tais como Declaração de Nascido Vivo (DNV), etiquetas de esterilização, capa do prontuário de internação, ficha de cirurgia descritiva, ficha de recuperação pós anestésica, ficha de identificação do recém-nascido e partograma.

O prontuário físico fica armazenado temporariamente na Central de Guias e é enviado para armazenamento no serviço terceirizado.

O gerenciamento, identificação, rastreabilidade e movimentação e acesso estão descritos em instrução IT-SAME-001 e PR-CEG-001. O serviço terceirizado de guarda de arquivo é qualificado e avaliado conforme política IT-ADM-002 e atende aos critérios de armazenamento, transporte e organização e sigilo das informações.

5.6. SEGURANÇA DO AMBIENTE LÓGICO

5.6.1. CONTROLE DE ACESSO AOS SISTEMAS (BASEADO EM SENHAS)

Na Unimed Sul Capixaba todos os usuários e aplicações que necessitem ter acesso a recursos são identificados e autenticados. Os usuários são responsáveis pelas suas ações executadas em suas contas.

As senhas de cada usuário são individuais, secretas, intransferíveis, sendo do colaborador ou das partes interessadas, a responsabilidade por garantir seu sigilo.

Os acessos aos sistemas são definidos através de perfis de acesso e as liberações são definidas de acordo com as necessidades de desempenho das funções (conforme definição do gestor da área) e considerando o princípio dos privilégios mínimos (ter acesso apenas aos recursos ou sistemas necessários para a execução das tarefas).

5.6.1.1. RESPONSABILIDADES DOS INDIVÍDUOS

Todo indivíduo com acesso a alguma aplicação da organização é responsável por elaborar senhas fortes, mantê-las seguras, e reportar qualquer uso não autorizado de suas contas conforme o Procedimento de Gestão de Controle de Acesso e Guarda de Registros de Conexão e Acesso (PR-INF-010).

5.6.1.2. RESPONSABILIDADES DA EQUIPE DE SEGURANÇA DA INFORMAÇÃO

A equipe de Segurança da Informação deve garantir que os requerimentos de senha sejam cumpridos para o acesso a qualquer aplicação ou dispositivo da organização ou dispositivo pessoal que seja utilizado para fins de acesso às aplicações corporativas conforme descrito no Procedimento de Gestão de Controle de Acesso e Guarda de Registros de Conexão e Acesso.

.

5.6.2. PRONTUÁRIO ELETRÔNICO (PEP)

O prontuário eletrônico é um conjunto de informações sobre o paciente contendo sua história de atendimentos e tratamentos. A elaboração do prontuário do paciente é um conjunto de registros multidisciplinares de admissões, prescrições de cuidados, exames, e medicamentos, protocolos e evoluções do paciente.

O prontuário eletrônico apresenta registros estruturados, com campos obrigatórios, a sua estrutura é definida por perfil de acesso para facilitar a visualização de informações mais necessárias.

Os acessos aos dados do PEP são restritos às áreas assistenciais diretamente ligadas ao processo de atendimento ao paciente e são amparados pelo sigilo profissional conforme destacado na Constituição Federal e nos Conselhos de Classe dos profissionais da saúde. Além disso, todo acesso só é realizado por meio de senha individual e intransferível e com registro de log de acessos.

5.6.3. REGISTRO DE EVENTOS

As informações (os registros propriamente ditos) são geradas e gravadas em banco de dados no momento do registro, preservando a informação da descrição do evento. Para a obtenção das informações necessárias foram definidos campos específicos nas telas de registros e tratamentos que permitem uma gestão em tempo real.

As informações geradas com o tratamento e gestão dos eventos são utilizadas pelas áreas e pelo Núcleo de Segurança do Paciente para tomadas de decisões e implantação de planos de ações.

5.6.4. USO DA INTERNET

A Unimed Sul Capixaba mantém regras de utilização e bloqueio de acesso a determinados sites, caixas de e-mail, conteúdos, anexos, emitentes, destinatários, limites de tráfegos e armazenamentos.
Desta forma, o uso e acesso à internet é restrito a sites relacionados as funções desempenhadas por cada colaborador.

A Unimed Sul Capixaba não autoriza a utilização dos meios de comunicação da cooperativa para divulgação de mensagens ou conteúdo ilegal, pornográfico, com qualquer sentido discriminatório, de cunho religioso, político-partidário, ideológico ou em desacordo com os princípios morais e éticos da cooperativa.

5.6.4.1. GUARDA DOS REGISTROS DE CONEXÃO E ACESSO

O acesso às redes, dispositivos, equipamentos e aplicações da organização deverá ser registrado e monitorado para identificar potencial má-utilização de sistemas, informações, dados pessoais ou dados pessoais sensíveis.

Os registros deverão ser mantidos seguros e passíveis de acesso somente por pessoal autorizado pela equipe da Tecnologia da Informação ou por quem ela expressamente determinar que realize a autorização.

5.6.5. CORREIO ELETRÔNICO/E-MAILS

O e-mail corporativo é uma ferramenta de trabalho, comunicação e apoio aos processos de negócios da Cooperativa, não podendo ser utilizado para fins pessoais. Com razão análoga, as informações de trabalho não podem ser trafegadas utilizando e-mails pessoais.

5.6.6. FERRAMENTAS DE COMUNICAÇÃO

A Unimed Sul Capixaba disponibiliza para uso de seus colaboradores ferramentas de troca de mensagens eletrônicas e o uso destas é exclusivamente para fins profissionais.

Fica terminantemente proibido o uso e a instalação de ferramentas de mensageria/comunicação on-line não homologados/autorizados pela equipe de TI.

5.7. SISTEMÁTICA DE BACKUP

A Unimed Sul Capixaba possui sistemática de backup apresentada no PR-INF-004, do Sistema de Gestão da Qualidade com o intuito de garantir a disponibilidade e a continuidade das informações. A Operadora possui um Plano de Continuidade de Negócios visando a manutenção das atividades em caso de catástrofes ou outras situações que possam afetar o funcionamento da Operadora.

5.8. RETENÇÃO E DESCARTE DE DOCUMENTOS

Os documentos e dados, inclusive pessoais, serão mantidos pelo tempo necessário para a atendimento de requisitos operacionais e legais, seguindo a temporalidade das tabelas de registro de cada setor da instituição.

5.8.1. DESTRUIÇÃO E ELIMINAÇÃO DOS DADOS

Ao final do período de temporalidade de armazenamento e desde que não exista uma razão válida para a manutenção das informações, os documentos contendo dados pessoais e/ou outra informação classificada como ultra confidencial ou confidencial que foram mantidos em cópias físicas serão destruídos como resíduo confidencial e aqueles mantidos eletronicamente serão eliminados dos sistemas da empresa conforme estabelecido no Procedimento de Retenção e Descarte de Registros Documentais e de Dados Pessoais (PR-SGQ-019).

5.9. MONITORAMENTO E AUDITORIA DO AMBIENTE

Para garantir as regras mencionadas nessa política, bem como assegurar que a mesma está sendo seguida, a UNIMED SUL CAPIXABA poderá:

- Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless dentre outros;
- Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior) ou por determinação da Diretoria da empresa;
- Identificar/nomear/discriminar usuários e seus respectivos acessos e/ou conversas;
- Executar, a qualquer tempo, inspeção física em regime de auditoria de segurança nas máquinas de sua propriedade, inclusive de forma esporádica e aleatória, no momento de um suporte e/ou manutenção de equipamentos.

5.10. VIGÊNCIA

Essa política será revisada anualmente ou em prazo inferior, sempre que houver necessidade de adequação das informações.

5.11. REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27001:2022 – Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos. Rio de Janeiro: ABNT, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27002:2022 – Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação. Rio de Janeiro: ABNT, 2022.

ISO/IEC. ISO/IEC 27005:2018 – Information technology – Security techniques – Information security risk management. Geneva: ISO, 2018.

NIST. SP 800-53 Rev. 5 – Security and Privacy Controls for Information Systems and Organizations. Gaithersburg: NIST, 2020. Disponível em: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5. Acesso em: 28 nov. 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União, Brasília, DF, 15 ago. 2018.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet). Diário Oficial da União, Brasília, DF, 24 abr. 2014.

BRASIL. Decreto nº 10.222, de 5 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética (E-Ciber). Diário Oficial da União, Brasília, DF, 6 fev. 2020.

6. REGRAS DE CONSEQUÊNCIAS

- Em caso de eventuais descumprimentos destas diretrizes, as consequências serão tratadas em conformidade com a legislação trabalhista, Estatuto Social e Código de Conduta da Unimed Sul Capixaba.

7. ANEXOS

- Não se aplica.